Amendments to the Claims:

This listing of claims will replace all prior versions and listings of claims in the application.

Listing of Claims:

1. (Currently Amended) A system for providing quarantine on a network comprising:

a client seeking access to a network resource;

a first server for providing the client with a manifest of checks and, if the manifest of checks is passed by the client, for providing the client proof that the client possesses a required configuration; and

a second server for providing access to the network resource, wherein the second server denies the client access to the network resource until the client presents the proof that the client possesses the required configuration;

wherein the client periodically requests that the proof be updated by the first server, regardless of further requests for access to the network resource.

2. (Original) The system of claim 1, wherein the checks include at least one of checks for installed software, a software version, an installed patch, an installed anti-virus system, an anti-virus state, a firewall state, an installed service, file sharing, a registry value, a registry key, and a file system state.

3. (Original) The system of claim 1, wherein the client comprises delegates that perform the checks in the manifest of checks.

4. (Previously Presented) The system of claim 1, wherein the client sends the first server the result the checks, and the first server provides the client with a certificate certifying that the client possesses the required configuration if the client passes the checks, and stores a copy of the certificate in a database.

5. (Original) The system of claim 4, wherein the client presents the certificate to the second server, and the second server validates the certificate by comparing the certificate to the copy of the certificate which is obtained from the first server.

6. (Canceled)

7. (Original) The system of claim 1, wherein if the client cannot provide proof that the client possesses the required configuration, the second server directs the client to the first server.

8. (Previously Presented) The system of claim 1, wherein the client sends the first server the result the checks, and the first server generates a certificate certifying that the client possesses the required configuration if the client passes the checks, and stores the certificate in a first database along with a unique identifier of the manifest of checks.

9. (Original) The system of claim 8, wherein the second server includes a second database that is a replica of the first database, wherein the client proves possession of the required configuration by sending the second server the unique identifier, wherein the second server compares the unique identifier to the unique identifier stored with the certificate in the second database.

10. (Original) The system of claim 1, wherein the first server requests a software inventory from the client and provides the client software necessary for the required configuration.

11. (Original) The system of claim 1, further comprising an access point for mediating communication between the client and the second server, wherein the second server is protected by a firewall.

12. (Original) The system of claim 1, wherein the first server is a service executing on a computing device and the second server is a service also executing on the computing device.

13. (Currently Amended) A method for a client to acquire access to a network resource, comprising:

receiving a manifest of checks from a first server, wherein the checks determine whether

the client possesses a required configuration;

performing the checks in the manifest of checks and sending the results of the checks to the first server;

receiving at the client proof of the required configuration from the first server;

requesting access to the network resource from a second server controlling access to the network resource; ~~and~~

sending from the client the proof of the required configuration to the second server; and

periodically requesting that the proof be updated by the first server, regardless of further requests for access to the network resource.

14. (Original) The method of claim 13, further comprising:

receiving a request for a software inventory from the first server; receiving software necessary for the required configuration; and installing the software.

15. (Original) The method of claim 13, further comprising:

sending results of the checks to the first server; and

receiving a certificate certifying that the client possesses a valid configuration.

16. (Original) The method of claim 15, further comprising presenting the certificate to the second server as proof of the required configuration.

17. (Original) The method of claim 13, wherein the proof is a unique identifier for the manifest.

18. (Original) The method of claim 13, wherein the first server is a service executing on a computing device and the second server is a service also executing on the computing device.

19.-22. (Canceled)

23. (Currently Amended) A method for quarantining a client from access to a network resource, comprising:

receiving at a first server a request for access to the network resource from the client;

receiving at the first server proof from the client of a required configuration;

validating at the first server the proof by comparing the proof to information obtained from a trusted server;

if the proof is valid, allowing access to the network resource; ~~and~~

if the proof is invalid, denying access to the network resource; and

periodically receiving a request that the proof be updated by the first server, regardless of further requests for access to the network resource.

24. (Original) The method of claim 23, further comprising, if the proof is invalid, directing the client to the trusted server so that the required configuration is obtained.

25. (Original) The method of claim 23, wherein the proof is a certificate, obtained from the trusted server, certifying that the client has the required configuration.

26. (Original) The method of claim 23, wherein the proof is a unique identifier for a manifest of checks that the client has performed.

27. (Canceled)

28. (Previously Presented) A computer program product for use in a computer system, the computer program product comprising one or more computer readable media having computer-executable instructions for implementing a method for a client to acquire access to a network resource, the method comprising the steps of:

receiving a manifest of checks from a first server, wherein the checks determine whether the client possesses a required configuration of installed software;

performing the checks in the manifest of checks and sending the results of the checks to the first server;

receiving at the client proof of the required configuration from the first server;

requesting access to the network resource from a second server controlling access to the network resource;

sending from the client the proof of the required configuration to the second server; and

periodically requesting that the proof be updated by the first server, regardless of further requests for access to the network resource.

29. (Currently Amended) A system for a client to acquire access to a network resource, comprising:

a processing unit; and

a memory coupled with and readable by the processing unit and having stored therein instructions which, when executed by the processing unit, cause a module to perform the following acts:

receiving a manifest of checks from a first server, wherein the checks determine whether the client possesses a required configuration;

performing the checks in the manifest of checks and sending the results of the checks to the first server;

receiving at the client proof of the required configuration from the first server;

storing the proof at the client;

requesting access to the network resource from a second server controlling access to the network resource;

determining whether the proof stored at the client is valid;

requesting, if the proof is no longer valid, the first server to update the proof; ~~and~~

sending from the client the proof of the required configuration to the second server; and

periodically requesting that the proof be updated by the first server, regardless of further requests for access to the network resource.